FIG. 1
(NETWORK COMMUNICATION SYSTEM)

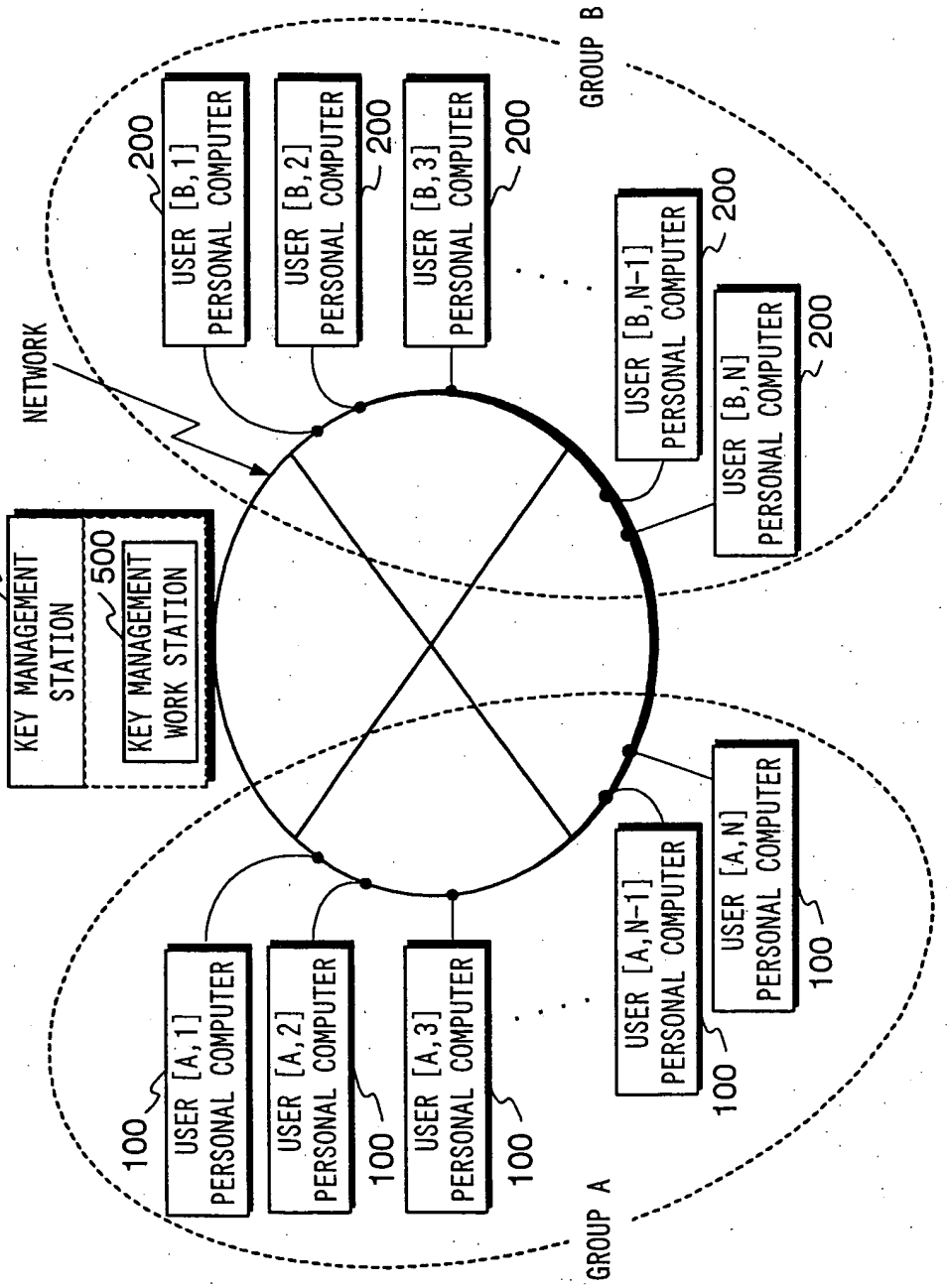


FIG. 2

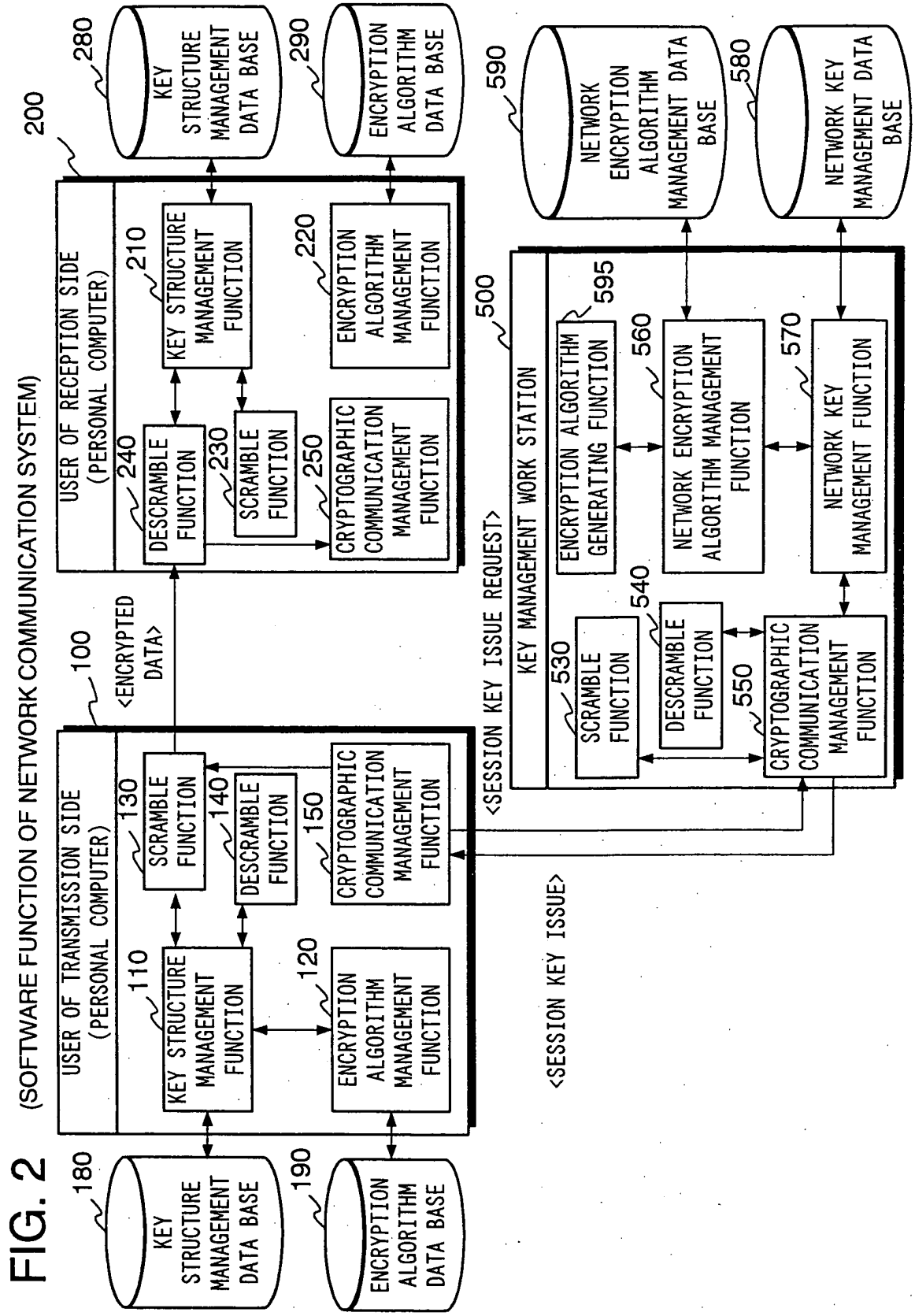

(SOFTWARE FUNCTION OF NETWORK COMMUNICATION SYSTEM)
USER OF TRANSMISSION SIDE (PERSONAL COMPUTER)
100
KEY STRUCTURE MANAGEMENT FUNCTION
110
ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
120
SCRAMBLE FUNCTION
130
DESCRAMBLE FUNCTION
140
CRYPTOGRAPHIC COMMUNICATION MANAGEMENT FUNCTION
150
KEY STRUCTURE MANAGEMENT DATA BASE
180
ENCRYPTION ALGORITHM DATA BASE
190
USER OF RECEPTION SIDE (PERSONAL COMPUTER)
200
KEY STRUCTURE MANAGEMENT FUNCTION
210
ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
220
SCRAMBLE FUNCTION
230
DESCRAMBLE FUNCTION
240
CRYPTOGRAPHIC COMMUNICATION MANAGEMENT FUNCTION
250
KEY STRUCTURE MANAGEMENT DATA BASE
280
ENCRYPTION ALGORITHM DATA BASE
290
<ENCRYPTED DATA>
<SESSION KEY ISSUE REQUEST>
<SESSION KEY ISSUE>
KEY MANAGEMENT WORK STATION
500
SCRAMBLE FUNCTION
530
DESCRAMBLE FUNCTION
540
CRYPTOGRAPHIC COMMUNICATION MANAGEMENT FUNCTION
550
NETWORK ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
560
NETWORK KEY MANAGEMENT FUNCTION
570
ENCRYPTION ALGORITHM GENERATING FUNCTION
595
NETWORK ENCRYPTION ALGORITHM MANAGEMENT DATA BASE
590
NETWORK KEY MANAGEMENT DATA BASE
580

FIG. 3A

NETWORK ENCRYPTION ALGORITHM MANAGEMENT DATA BASE

USER ID	ENCRYPTION ALGORITHM NAME	ENCRYPTION ALGORITHM VERSION	UPDATING DATE
KEY MANAGEMENT STATION ID	ENCRYPTION ALGORITHM NAME	ENCRYPTION ALGORITHM VERSION	UPDATING DATE

FIG. 3B

NETWORK KEY MANAGEMENT DATA BASE

USER ID	ENCRYPTION ALGORITHM NAME	ENCRYPTION ALGORITHM VERSION	KEY INFORMATION	UPDATING DATE
KEY MANAGEMENT STATION ID	ENCRYPTION ALGORITHM NAME	ENCRYPTION ALGORITHM VERSION	KEY INFORMATION	UPDATING DATE

FIG. 4A

ENCRYPTION ALGORITHM MANAGEMENT DATA BASE

ENCRYPTION ALGORITHM NAME	ENCRYPTION ALGORITHM VERSION	UPDATING DATE

FIG. 4B

KEY STRUCTURE MANAGEMENT DATA BASE

ENCRYPTION ALGORITHM NAME	ENCRYPTION ALGORITHM VERSION	USER KEY INFORMATION	UPDATING DATE
ENCRYPTION ALGORITHM NAME	ENCRYPTION ALGORITHM VERSION	KEY INFORMATION OF KEY MANAGEMENT STATION	UPDATING DATE

FIG. 5

(OUTLINE OF ENCRYPTION ALGORITHM CONVERSION)

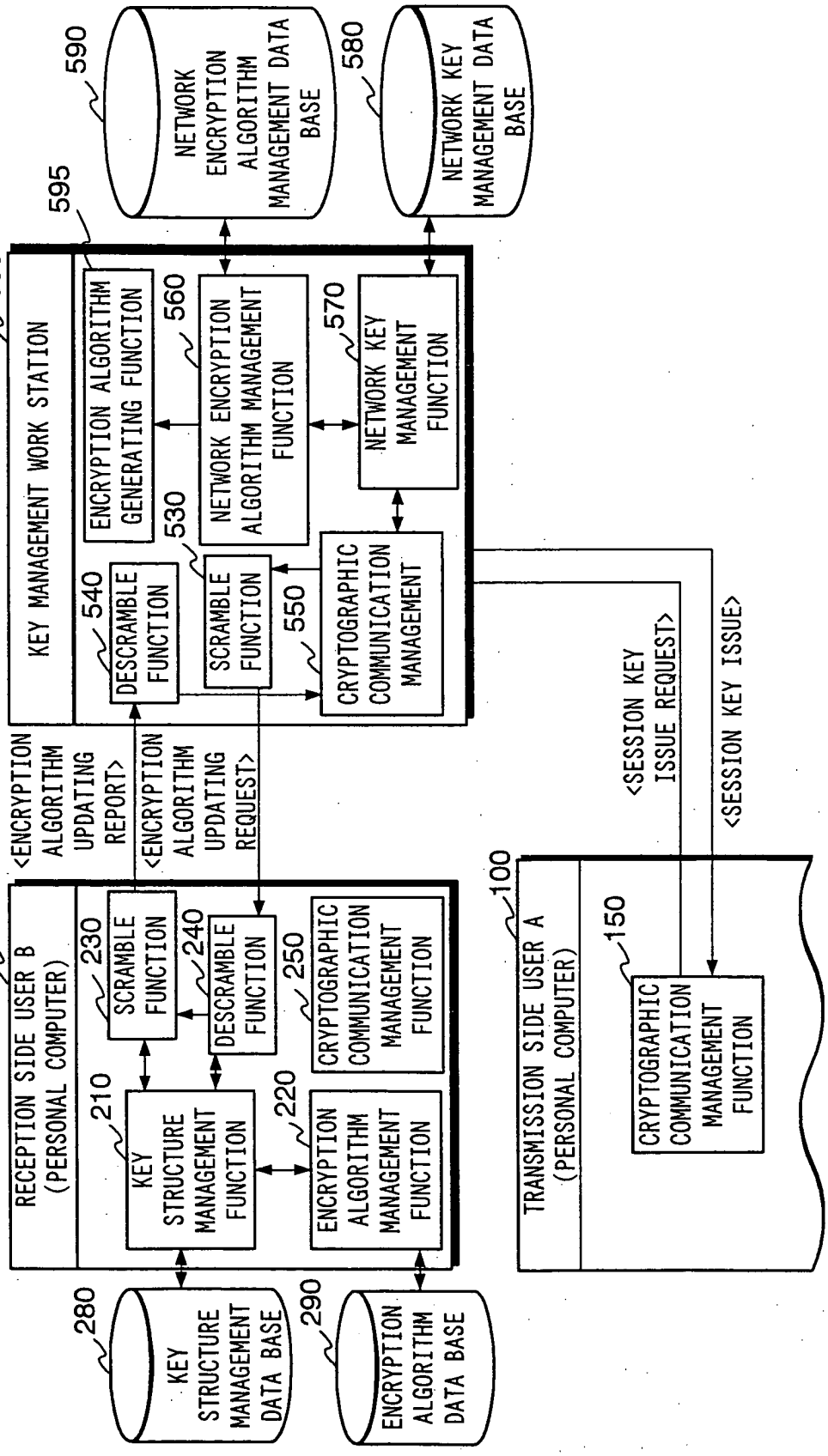


FIG. 6

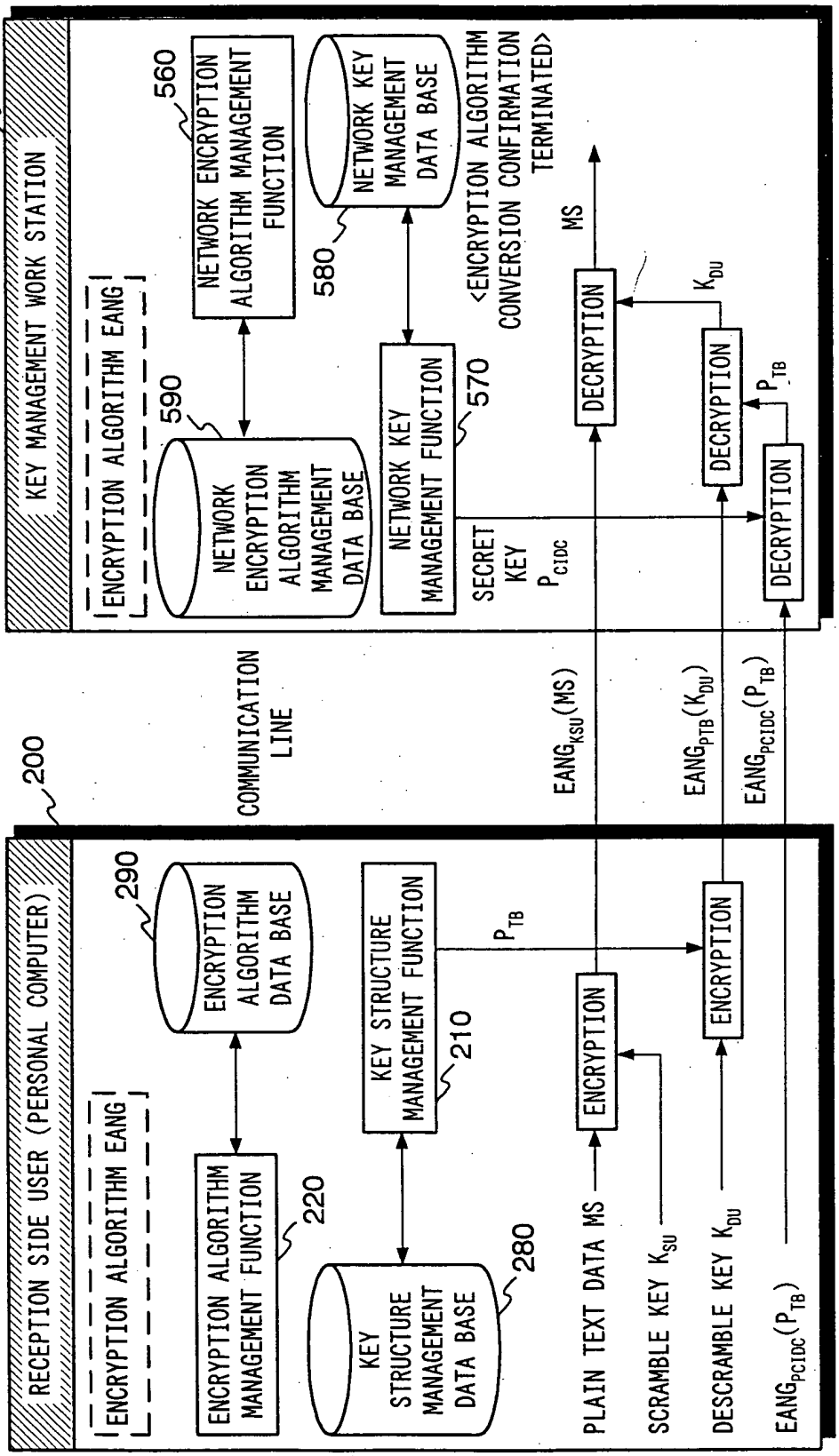

500
KEY MANAGEMENT WORK STATION
ENCRYPTION ALGORITHM EANG
NETWORK ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
560
NETWORK KEY MANAGEMENT DATA BASE
580
NETWORK ENCRYPTION ALGORITHM MANAGEMENT DATA BASE
590
NETWORK KEY MANAGEMENT FUNCTION
570
SECRET KEY P_{CIDC}
<ENCRYPTION ALGORITHM CONVERSION CONFIRMATION TERMINATED>
DECRYPTION
MS
K_{DU}
DECRYPTION
P_{TB}
DECRYPTION
COMMUNICATION LINE
$EANG_{KSU}(MS)$
$EANG_{PTB}(K_{DU})$
$EANG_{PCIDC}(P_{TB})$
200
RECEPTION SIDE USER (PERSONAL COMPUTER)
ENCRYPTION ALGORITHM EANG
ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
220
ENCRYPTION ALGORITHM DATA BASE
290
KEY STRUCTURE MANAGEMENT FUNCTION
210
P_{TB}
KEY STRUCTURE MANAGEMENT DATA BASE
280
ENCRYPTION
ENCRYPTION
PLAIN TEXT DATA MS
SCRAMBLE KEY K_{SU}
DESCRAMBLE KEY K_{DU}
$EANG_{PCIDC}(P_{TB})$

FIG. 7

(CRYPTOGRAPHIC COMMUNICATION BY COMMON KEY CIPHER)

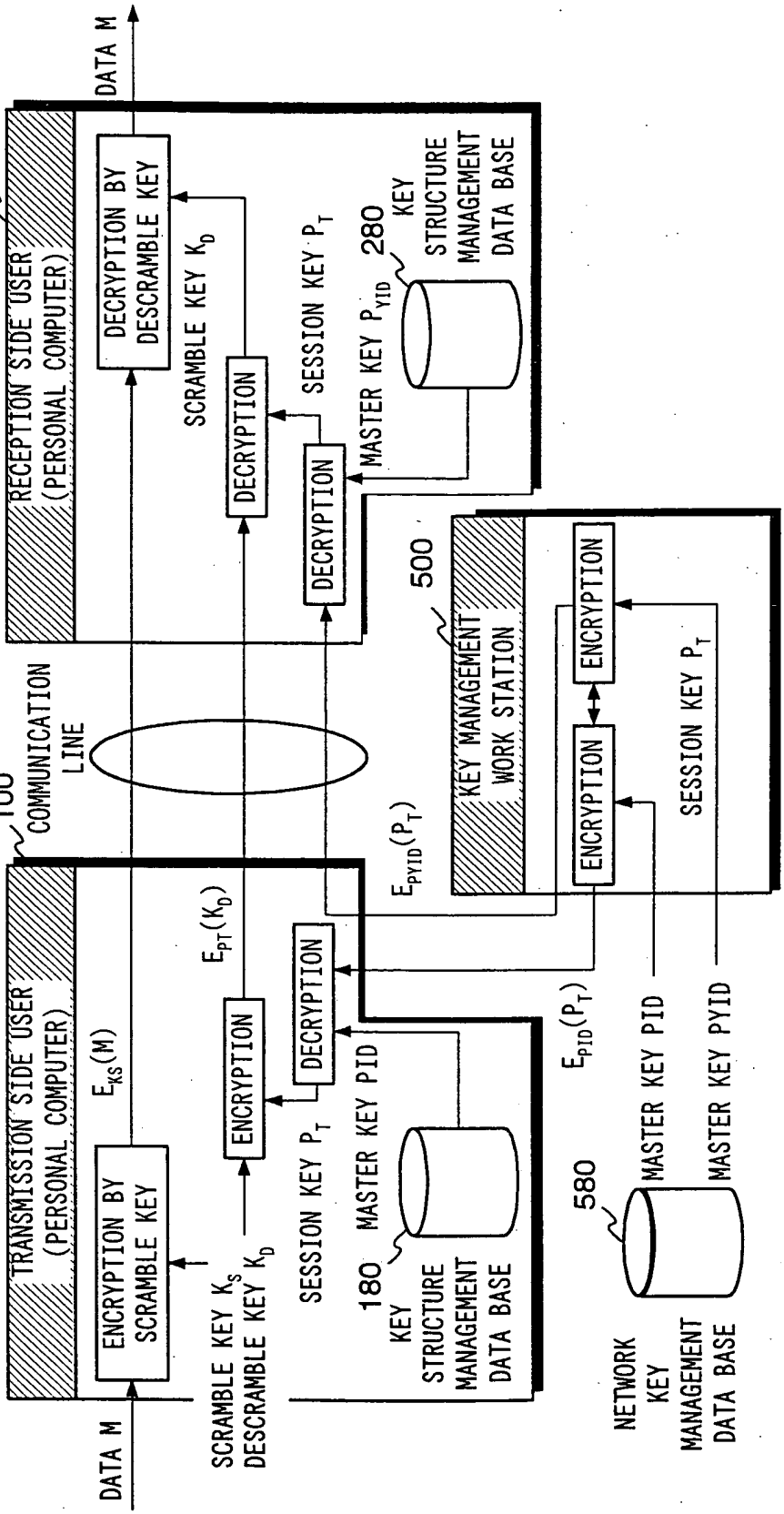


FIG. 8

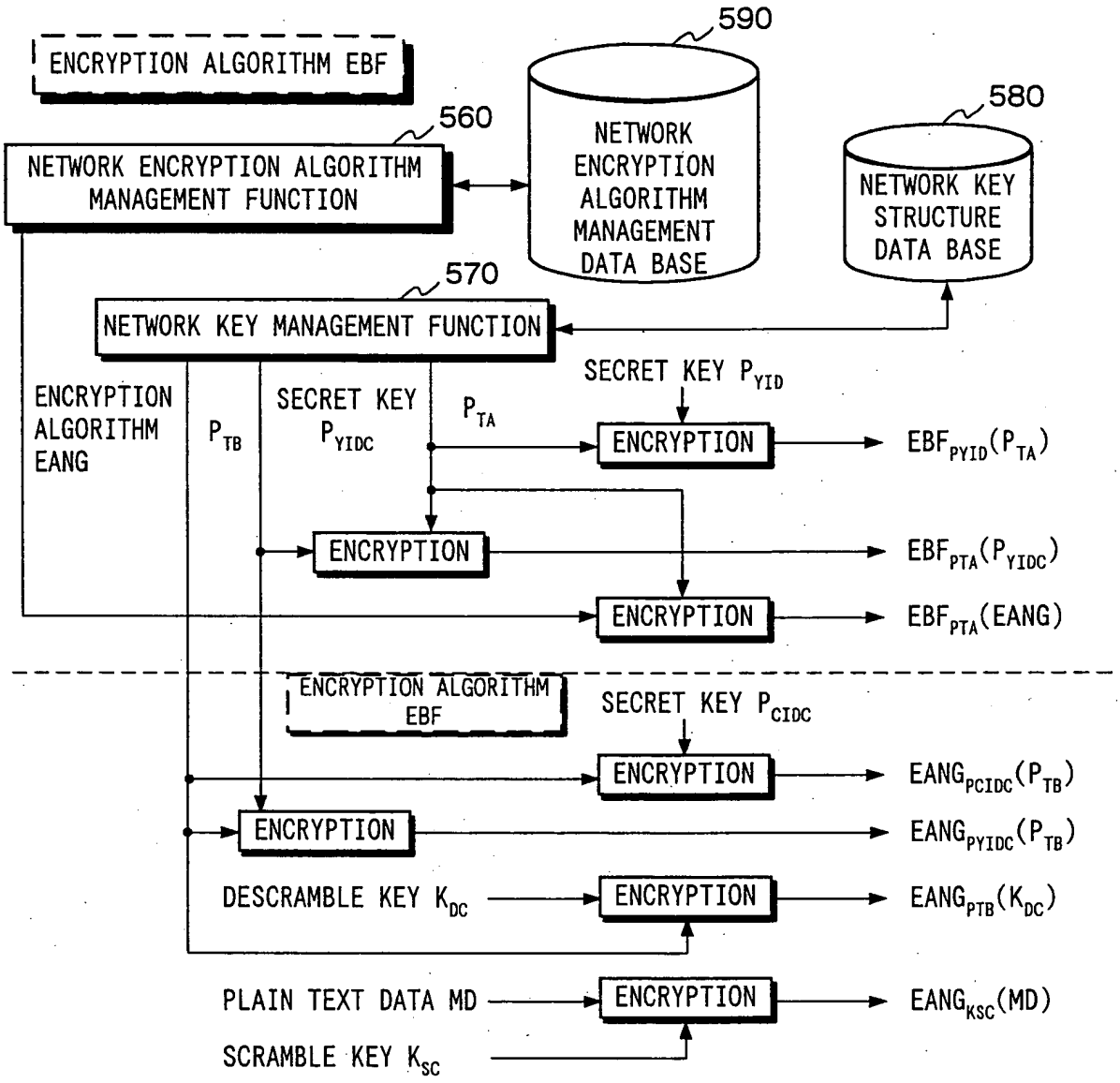

590
ENCRYPTION ALGORITHM EBF
560
NETWORK ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
NETWORK ENCRYPTION ALGORITHM MANAGEMENT DATA BASE
580
NETWORK KEY STRUCTURE DATA BASE
570
NETWORK KEY MANAGEMENT FUNCTION
SECRET KEY P_{YID}
ENCRYPTION ALGORITHM EANG
P_{TB}
SECRET KEY P_{YIDC}
P_{TA}
ENCRYPTION
$EBF_{PYID}(P_{TA})$
ENCRYPTION
$EBF_{PTA}(P_{YIDC})$
ENCRYPTION
$EBF_{PTA}(EANG)$
ENCRYPTION ALGORITHM EBF
SECRET KEY P_{CIDC}
ENCRYPTION
$EANG_{PCIDC}(P_{TB})$
ENCRYPTION
$EANG_{PYIDC}(P_{TB})$
DESCRAMBLE KEY K_{DC}
ENCRYPTION
$EANG_{PTB}(K_{DC})$
PLAIN TEXT DATA MD
ENCRYPTION
$EANG_{KSC}(MD)$
SCRAMBLE KEY K_{SC}

FIG. 9

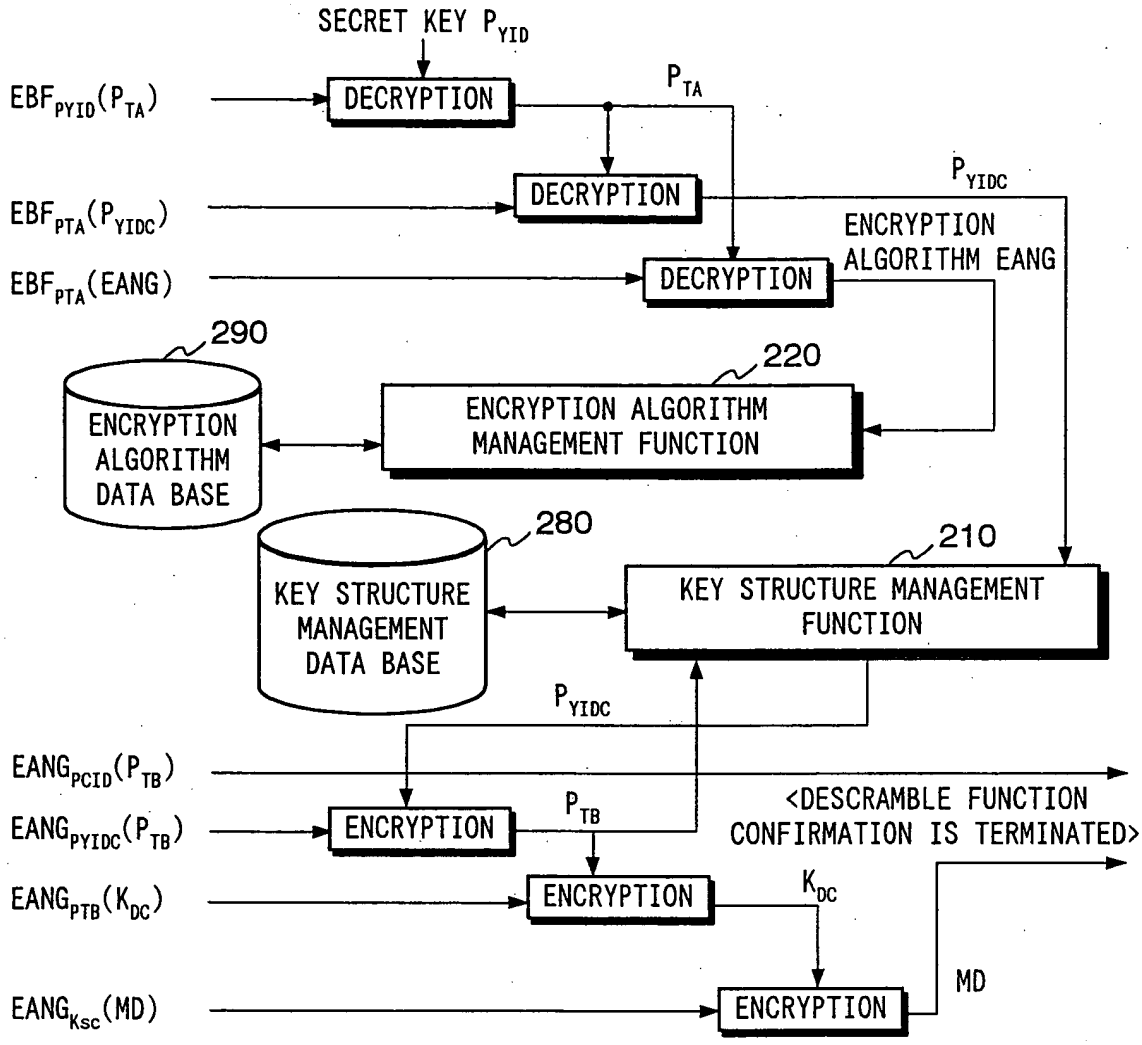
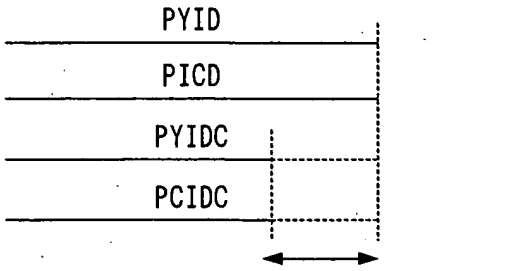
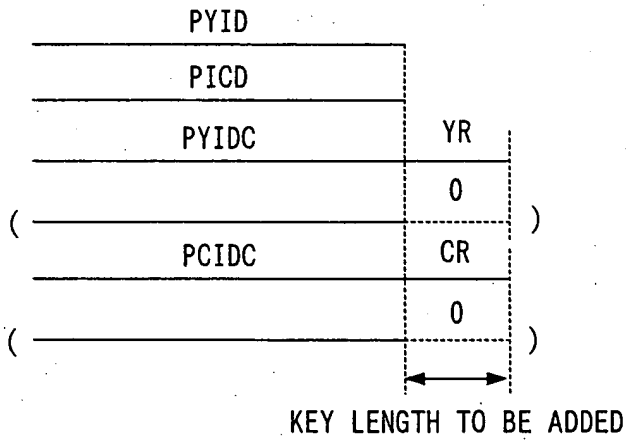

SECRET KEY P_{YID}
$EBF_{PYID}(P_{TA})$
DECRYPTION
P_{TA}
$EBF_{PTA}(P_{YIDC})$
DECRYPTION
P_{YIDC}
$EBF_{PTA}(EANG)$
DECRYPTION
ENCRYPTION ALGORITHM EANG
290
ENCRYPTION ALGORITHM DATA BASE
220
ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
280
KEY STRUCTURE MANAGEMENT DATA BASE
210
KEY STRUCTURE MANAGEMENT FUNCTION
P_{YIDC}
$EANG_{PCID}(P_{TB})$
$EANG_{PYIDC}(P_{TB})$
ENCRYPTION
P_{TB}
<DESCRAMBLE FUNCTION CONFIRMATION IS TERMINATED>
$EANG_{PTB}(K_{DC})$
ENCRYPTION
K_{DC}
$EANG_{Ksc}(MD)$
ENCRYPTION
MD

FIG. 10A



CASE WHERE THE KEY LENGTH IS SHORTENED

FIG. 10B



CASE WHERE THE KEY LENGTH IS PROLONGED

FIG. 11

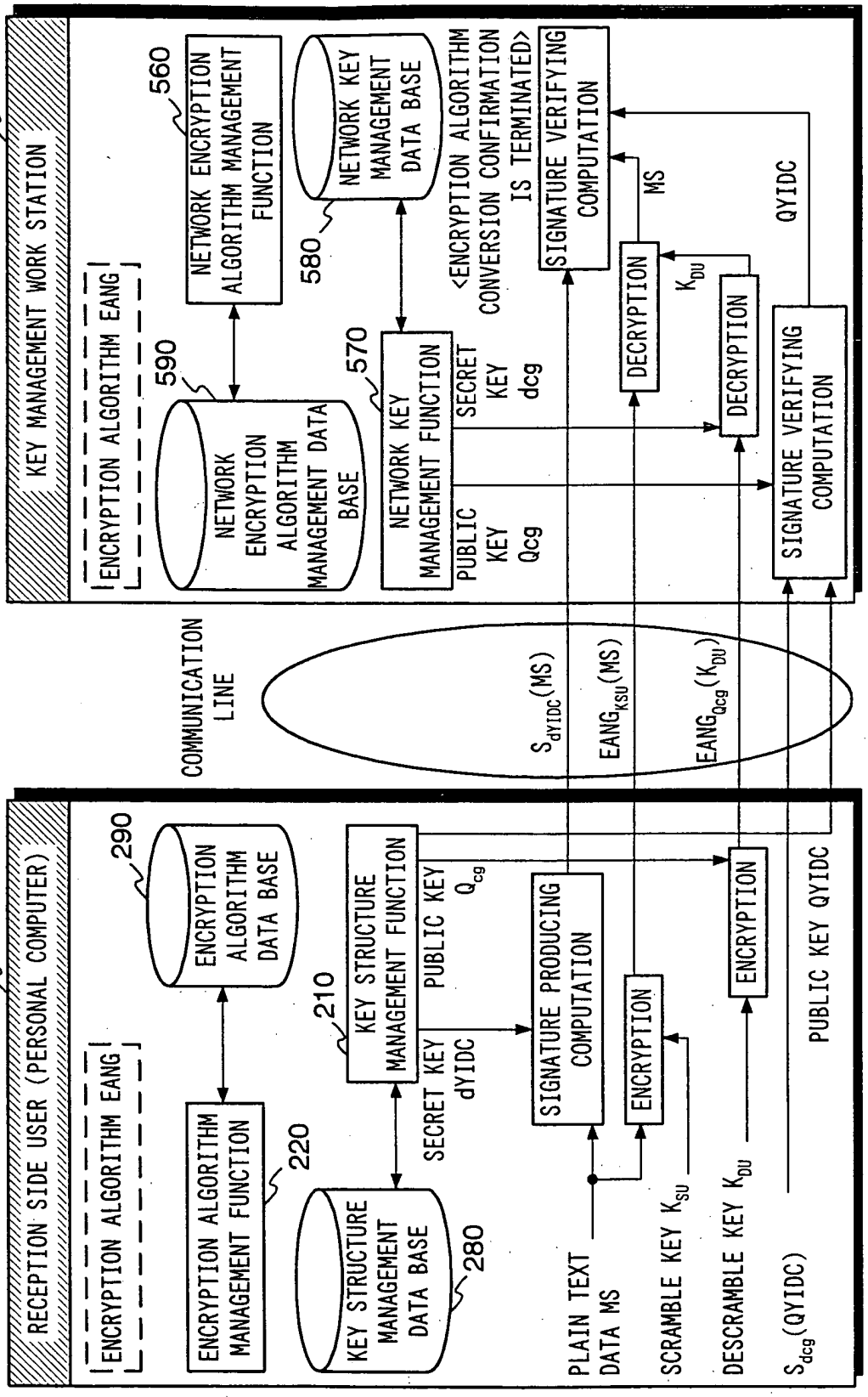

500
KEY MANAGEMENT WORK STATION
ENCRYPTION ALGORITHM EANG
560
NETWORK ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
580
NETWORK KEY MANAGEMENT DATA BASE
590
NETWORK ENCRYPTION ALGORITHM MANAGEMENT DATA BASE
570
NETWORK KEY MANAGEMENT FUNCTION
PUBLIC KEY Qcg
SECRET KEY dcg
<ENCRYPTION ALGORITHM CONVERSION CONFIRMATION IS TERMINATED>
SIGNATURE VERIFYING COMPUTATION
DECRYPTION
MS
K_{DU}
DECRYPTION
QYIDC
SIGNATURE VERIFYING COMPUTATION
COMMUNICATION LINE
S_{dYIDC}(MS)
$EANG_{KSU}$(MS)
$EANG_{Qcg}$(K_{DU})
200
RECEPTION SIDE USER (PERSONAL COMPUTER)
ENCRYPTION ALGORITHM EANG
ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
220
290
ENCRYPTION ALGORITHM DATA BASE
210
KEY STRUCTURE MANAGEMENT FUNCTION
PUBLIC KEY Q_{cg}
SECRET KEY dYIDC
KEY STRUCTURE MANAGEMENT DATA BASE
280
SIGNATURE PRODUCING COMPUTATION
ENCRYPTION
ENCRYPTION
PLAIN TEXT DATA MS
SCRAMBLE KEY K_{SU}
DESCRAMBLE KEY K_{DU}
S_{dcg}(QYIDC)
PUBLIC KEY QYIDC

FIG. 12

(CRYPTOGRAPHIC COMMUNICATION BY PUBLIC KEY CIPHER)

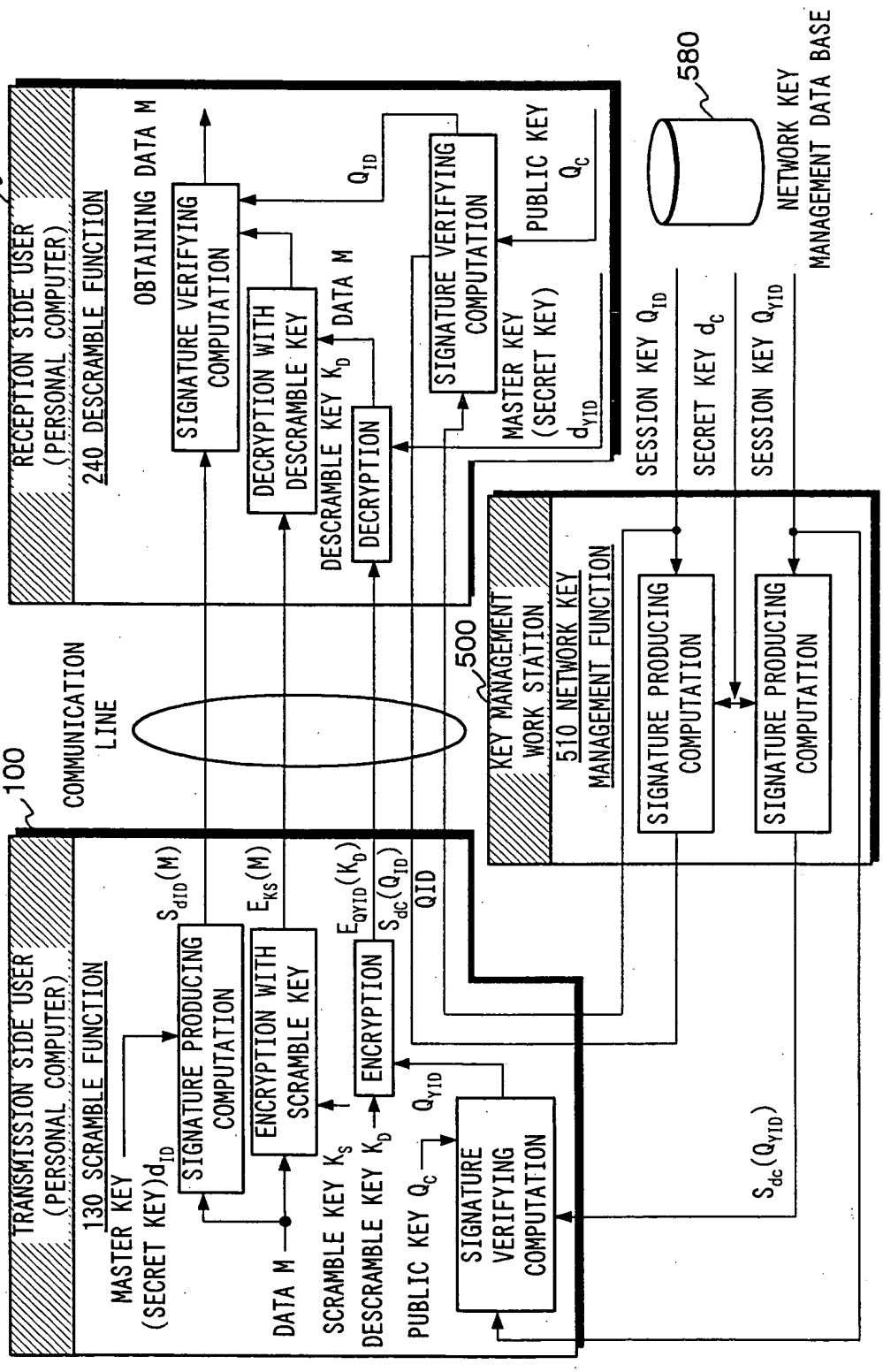


FIG. 13

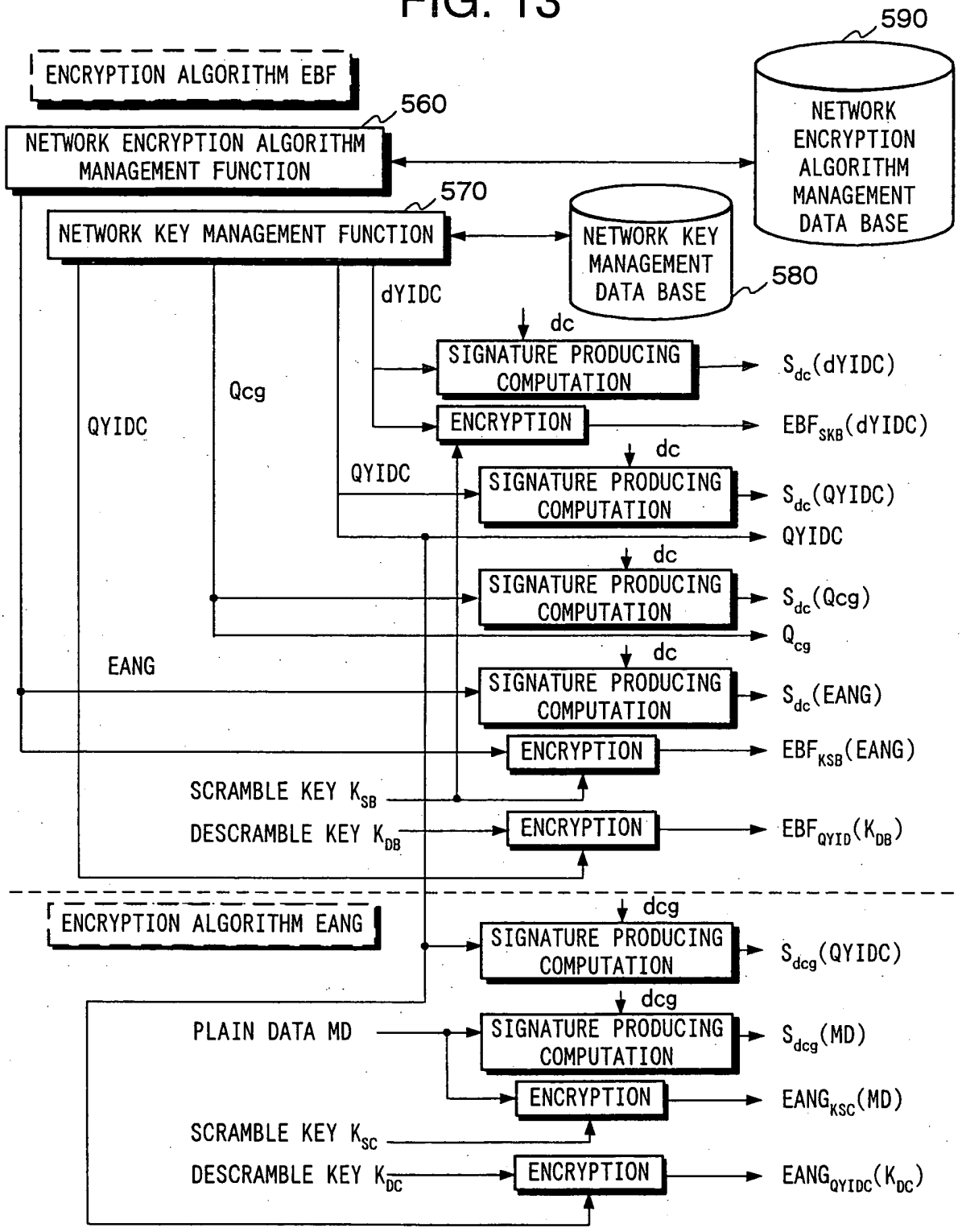

590
ENCRYPTION ALGORITHM EBF
560
NETWORK ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
NETWORK ENCRYPTION ALGORITHM MANAGEMENT DATA BASE
570
NETWORK KEY MANAGEMENT FUNCTION
NETWORK KEY MANAGEMENT DATA BASE
580
dYIDC
dc
SIGNATURE PRODUCING COMPUTATION
S_{dc}(dYIDC)
Qcg
ENCRYPTION
EBF_{SKB}(dYIDC)
QYIDC
dc
QYIDC
SIGNATURE PRODUCING COMPUTATION
S_{dc}(QYIDC)
QYIDC
dc
SIGNATURE PRODUCING COMPUTATION
S_{dc}(Qcg)
Q_{cg}
dc
EANG
SIGNATURE PRODUCING COMPUTATION
S_{dc}(EANG)
ENCRYPTION
EBF_{KSB}(EANG)
SCRAMBLE KEY K_{SB}
DESCRAMBLE KEY K_{DB}
ENCRYPTION
EBF_{QYID}(K_{DB})
ENCRYPTION ALGORITHM EANG
dcg
SIGNATURE PRODUCING COMPUTATION
S_{dcg}(QYIDC)
dcg
PLAIN DATA MD
SIGNATURE PRODUCING COMPUTATION
S_{dcg}(MD)
ENCRYPTION
$EANG_{KSC}$(MD)
SCRAMBLE KEY K_{SC}
DESCRAMBLE KEY K_{DC}
ENCRYPTION
$EANG_{QYIDC}$(K_{DC})

FIG. 14

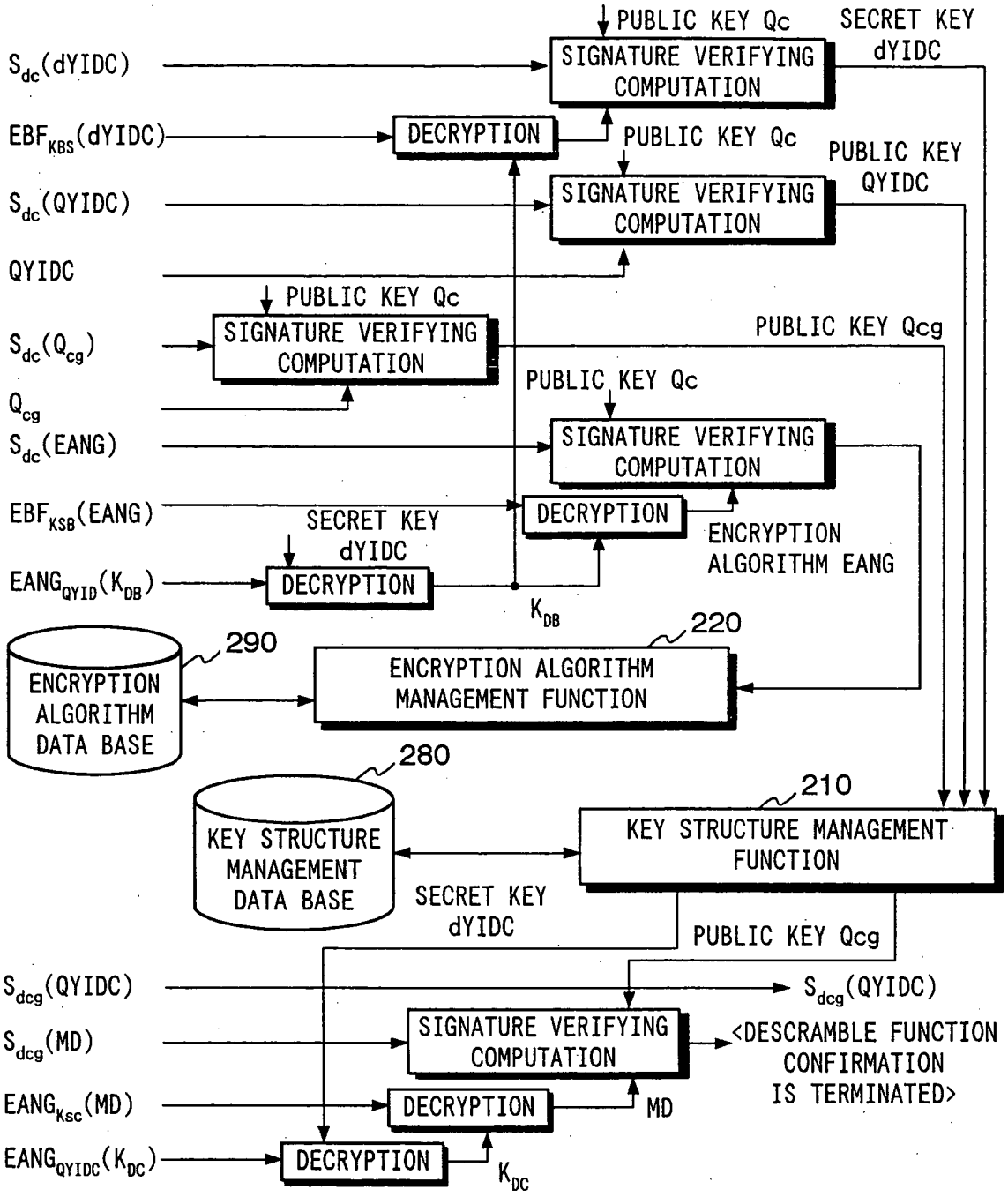

PUBLIC KEY Qc
SECRET KEY dYIDC
S_{dc}(dYIDC)
SIGNATURE VERIFYING COMPUTATION
EBF_{KBS}(dYIDC)
DECRYPTION
PUBLIC KEY Qc
PUBLIC KEY QYIDC
S_{dc}(QYIDC)
SIGNATURE VERIFYING COMPUTATION
QYIDC
PUBLIC KEY Qc
S_{dc}(Q_{cg})
SIGNATURE VERIFYING COMPUTATION
PUBLIC KEY Qcg
Q_{cg}
PUBLIC KEY Qc
S_{dc}(EANG)
SIGNATURE VERIFYING COMPUTATION
EBF_{KSB}(EANG)
DECRYPTION
ENCRYPTION ALGORITHM EANG
SECRET KEY dYIDC
$EANG_{QYID}$(K_{DB})
DECRYPTION
K_{DB}
290
ENCRYPTION ALGORITHM DATA BASE
220
ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
280
210
KEY STRUCTURE MANAGEMENT DATA BASE
KEY STRUCTURE MANAGEMENT FUNCTION
SECRET KEY dYIDC
PUBLIC KEY Qcg
S_{dcg}(QYIDC)
S_{dcg}(QYIDC)
S_{dcg}(MD)
SIGNATURE VERIFYING COMPUTATION
<DESCRAMBLE FUNCTION CONFIRMATION IS TERMINATED>
$EANG_{Ksc}$(MD)
DECRYPTION
MD
$EANG_{QYIDC}$(K_{DC})
DECRYPTION
K_{DC}

FIG. 15

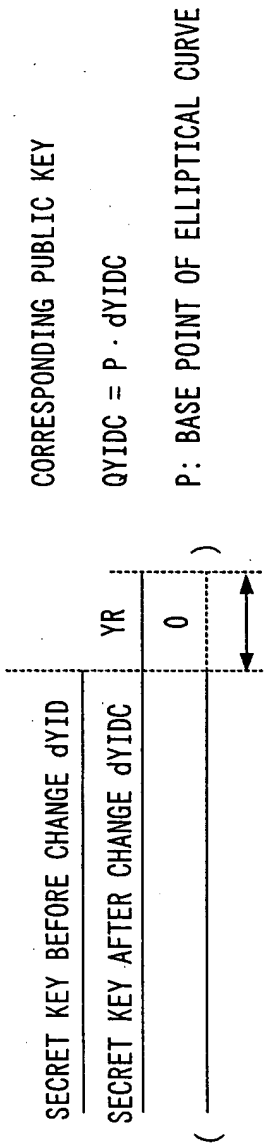

CORRESPONDING PUBLIC KEY
QYIDC = P · dYIDC
P: BASE POINT OF ELLIPTICAL CURVE
SECRET KEY BEFORE CHANGE dYID
SECRET KEY AFTER CHANGE dYIDC
YR
0
KEY LENGTH TO BE ADDED

FIG. 16

(CRYPTOGRAPHIC COMMUNICATION SYSTEM BASED ON PUBLIC KEY ENCRYPTION ALGORITHM)

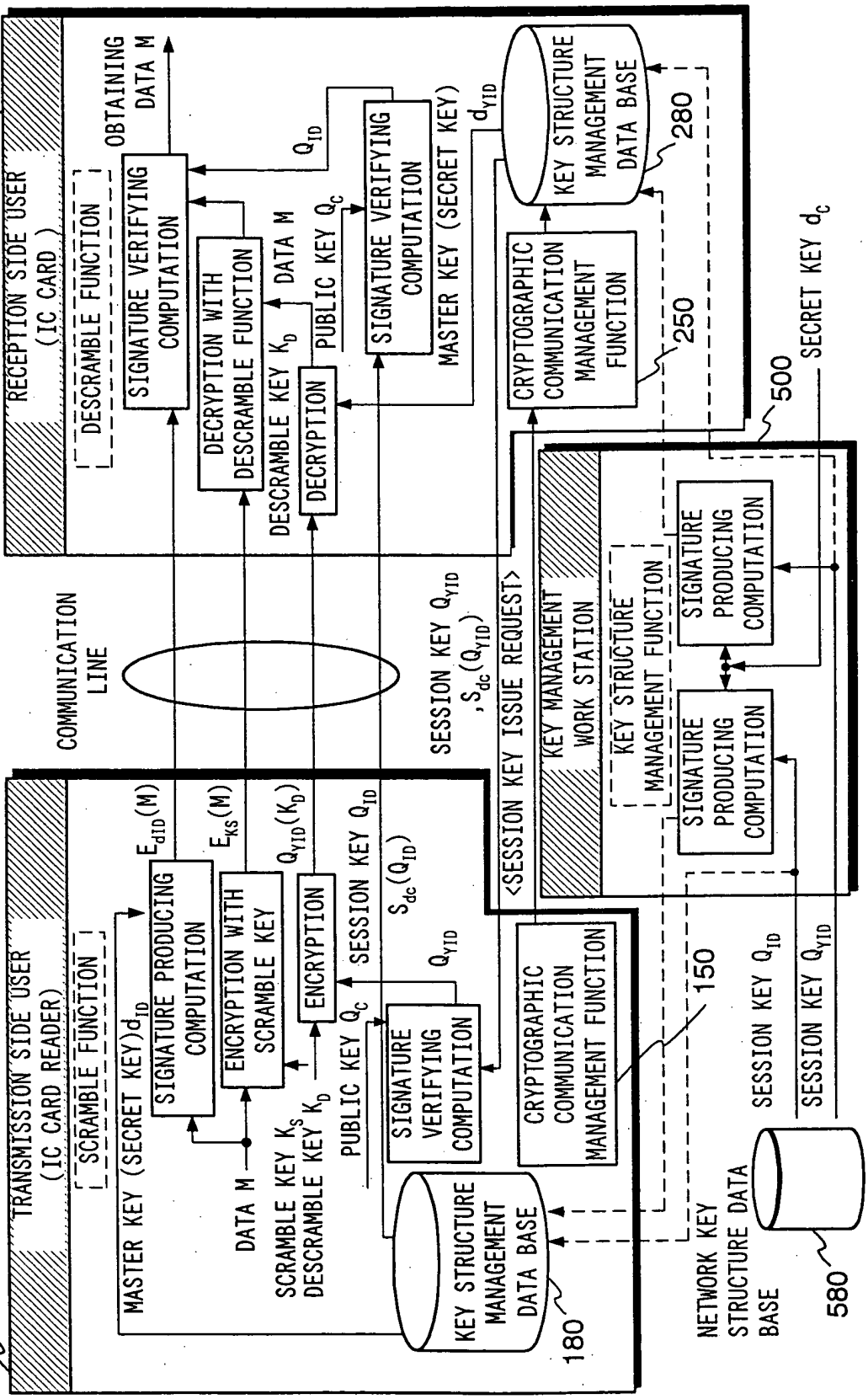


FIG. 17 (ALGORITHM CONVERSION OF PORTABLE INFORMATION PROCESSING UNIT)

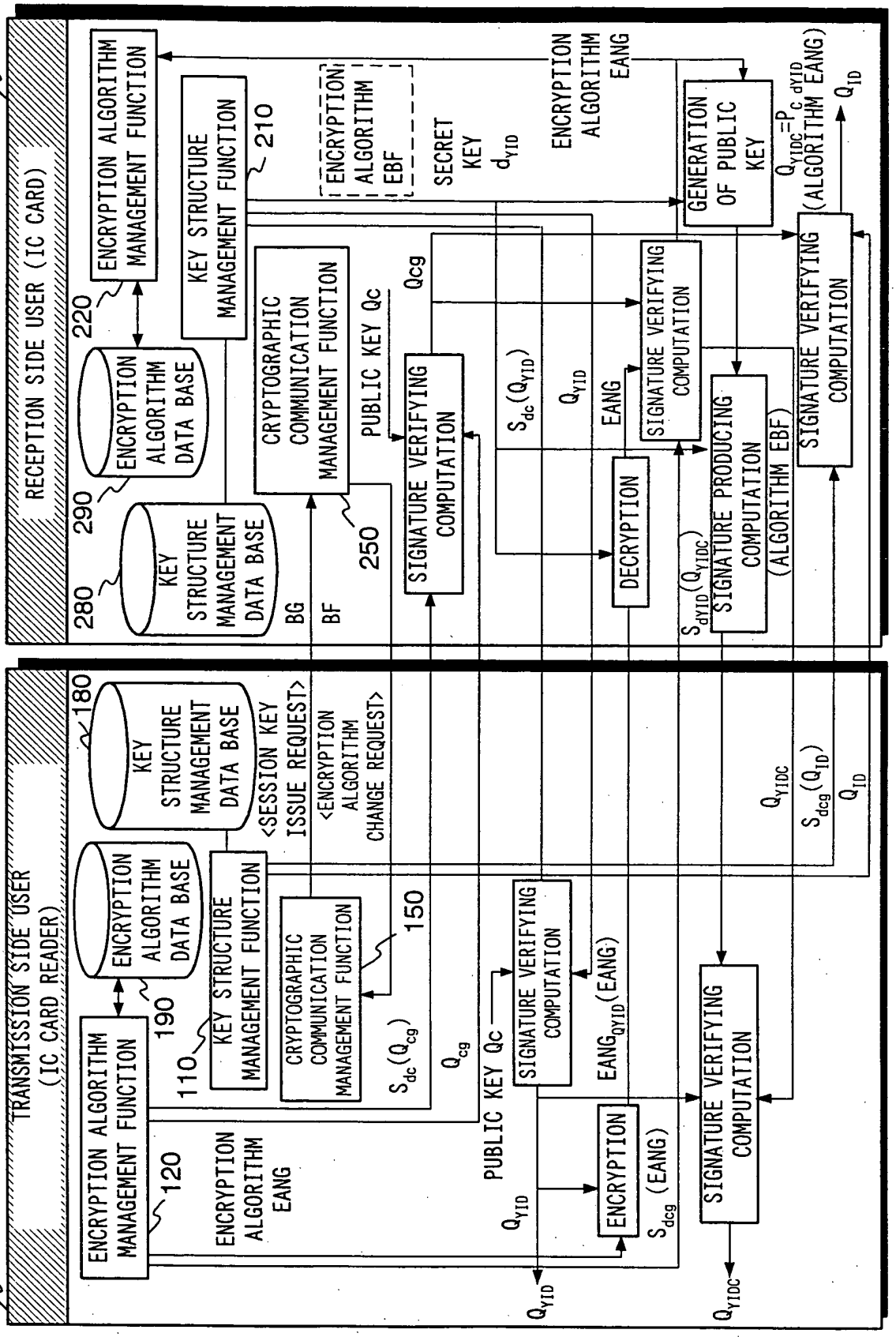


FIG. 18

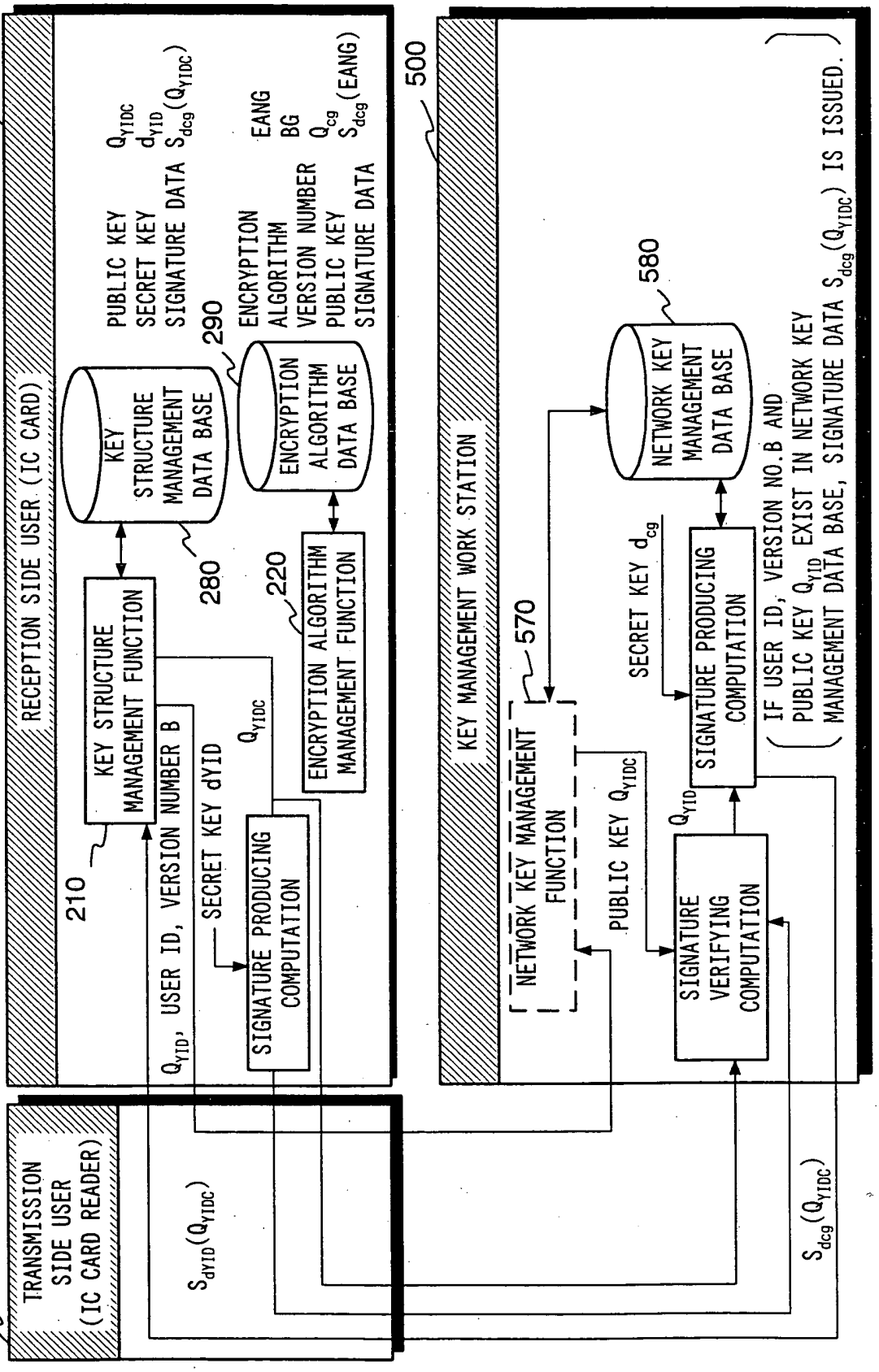

(ALGORITHM CONVERSION OF PORTABLE INFORMATION PROCESSING UNIT)
100
TRANSMISSION SIDE USER (IC CARD READER)
200
RECEPTION SIDE USER (IC CARD)
210
KEY STRUCTURE MANAGEMENT FUNCTION
280
KEY STRUCTURE MANAGEMENT DATA BASE
PUBLIC KEY Q_{YIDC}
SECRET KEY d_{YID}
SIGNATURE DATA $S_{dcg}(Q_{YIDC})$
290
ENCRYPTION ALGORITHM DATA BASE
ENCRYPTION ALGORITHM VERSION NUMBER
PUBLIC KEY
SIGNATURE DATA
EANG
BG
Q_{cg}
$S_{dcg}(EANG)$
220
ENCRYPTION ALGORITHM MANAGEMENT FUNCTION
Q_{YID}, USER ID, VERSION NUMBER B
SECRET KEY dYID
Q_{YIDC}
SIGNATURE PRODUCING COMPUTATION
$S_{dYID}(Q_{YIDC})$
500
KEY MANAGEMENT WORK STATION
570
NETWORK KEY MANAGEMENT FUNCTION
PUBLIC KEY Q_{YIDC}
SECRET KEY d_{cg}
580
NETWORK KEY MANAGEMENT DATA BASE
Q_{YID}
SIGNATURE PRODUCING COMPUTATION
SIGNATURE VERIFYING COMPUTATION
$S_{dcg}(Q_{YIDC})$
IF USER ID, VERSION NO.B AND PUBLIC KEY Q_{YID} EXIST IN NETWORK KEY MANAGEMENT DATA BASE, SIGNATURE DATA $S_{dcg}(Q_{YIDC})$ IS ISSUED.

FIG. 19

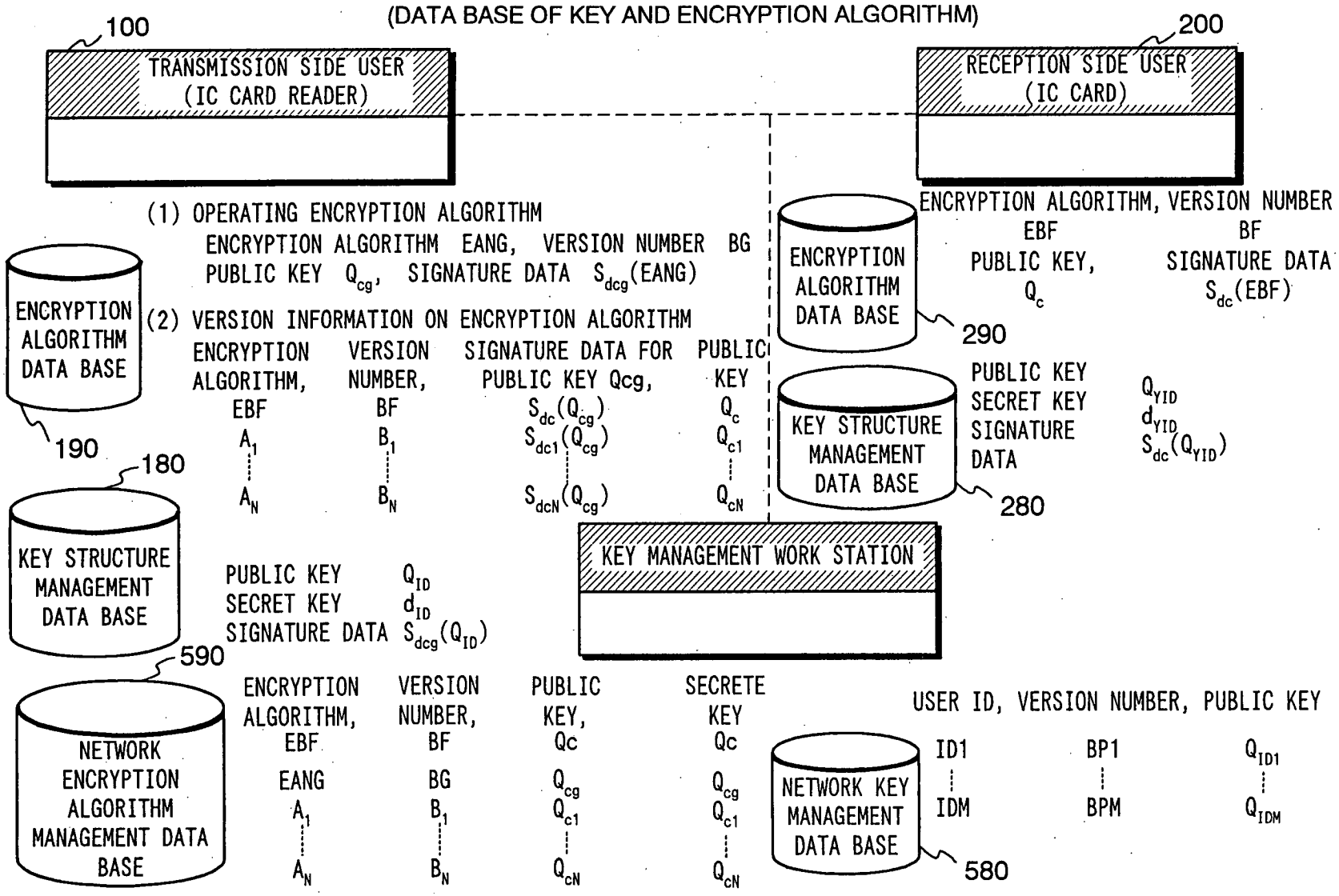

(DATA BASE OF KEY AND ENCRYPTION ALGORITHM)
100
TRANSMISSION SIDE USER
(IC CARD READER)
200
RECEPTION SIDE USER
(IC CARD)
(1) OPERATING ENCRYPTION ALGORITHM
ENCRYPTION ALGORITHM EANG, VERSION NUMBER BG
PUBLIC KEY Q_{cg}, SIGNATURE DATA S_{dcg}(EANG)
(2) VERSION INFORMATION ON ENCRYPTION ALGORITHM
ENCRYPTION ALGORITHM, EBF
VERSION NUMBER, BF
SIGNATURE DATA FOR PUBLIC KEY Qcg, $S_{dc}(Q_{cg})$
PUBLIC KEY Q_c
A_1 ... A_N
B_1 ... B_N
$S_{dc1}(Q_{cg})$ ... $S_{dcN}(Q_{cg})$
Q_{c1} ... Q_{cN}
ENCRYPTION ALGORITHM DATA BASE
190
180
KEY STRUCTURE MANAGEMENT DATA BASE
PUBLIC KEY Q_{ID}
SECRET KEY d_{ID}
SIGNATURE DATA $S_{dcg}(Q_{ID})$
590
NETWORK ENCRYPTION ALGORITHM MANAGEMENT DATA BASE
ENCRYPTION ALGORITHM, EBF
VERSION NUMBER, BF
PUBLIC KEY, Qc
SECRETE KEY Qc
EANG
A_1 ... A_N
BG
B_1 ... B_N
Q_{cg}
Q_{c1} ... Q_{cN}
Q_{cg}
Q_{c1} ... Q_{cN}
KEY MANAGEMENT WORK STATION
ENCRYPTION ALGORITHM DATA BASE
290
ENCRYPTION ALGORITHM, VERSION NUMBER
EBF
PUBLIC KEY, Q_c
BF
SIGNATURE DATA S_{dc}(EBF)
KEY STRUCTURE MANAGEMENT DATA BASE
280
PUBLIC KEY Q_{YID}
SECRET KEY d_{YID}
SIGNATURE DATA $S_{dc}(Q_{YID})$
NETWORK KEY MANAGEMENT DATA BASE
580
USER ID, VERSION NUMBER, PUBLIC KEY
ID1 ... IDM
BP1 ... BPM
Q_{ID1} ... Q_{IDM}

FIG. 20

(ENCRYPTION ALGORITHM CONVERSION FOR USER TO GENERATE HIS OWN KEY)

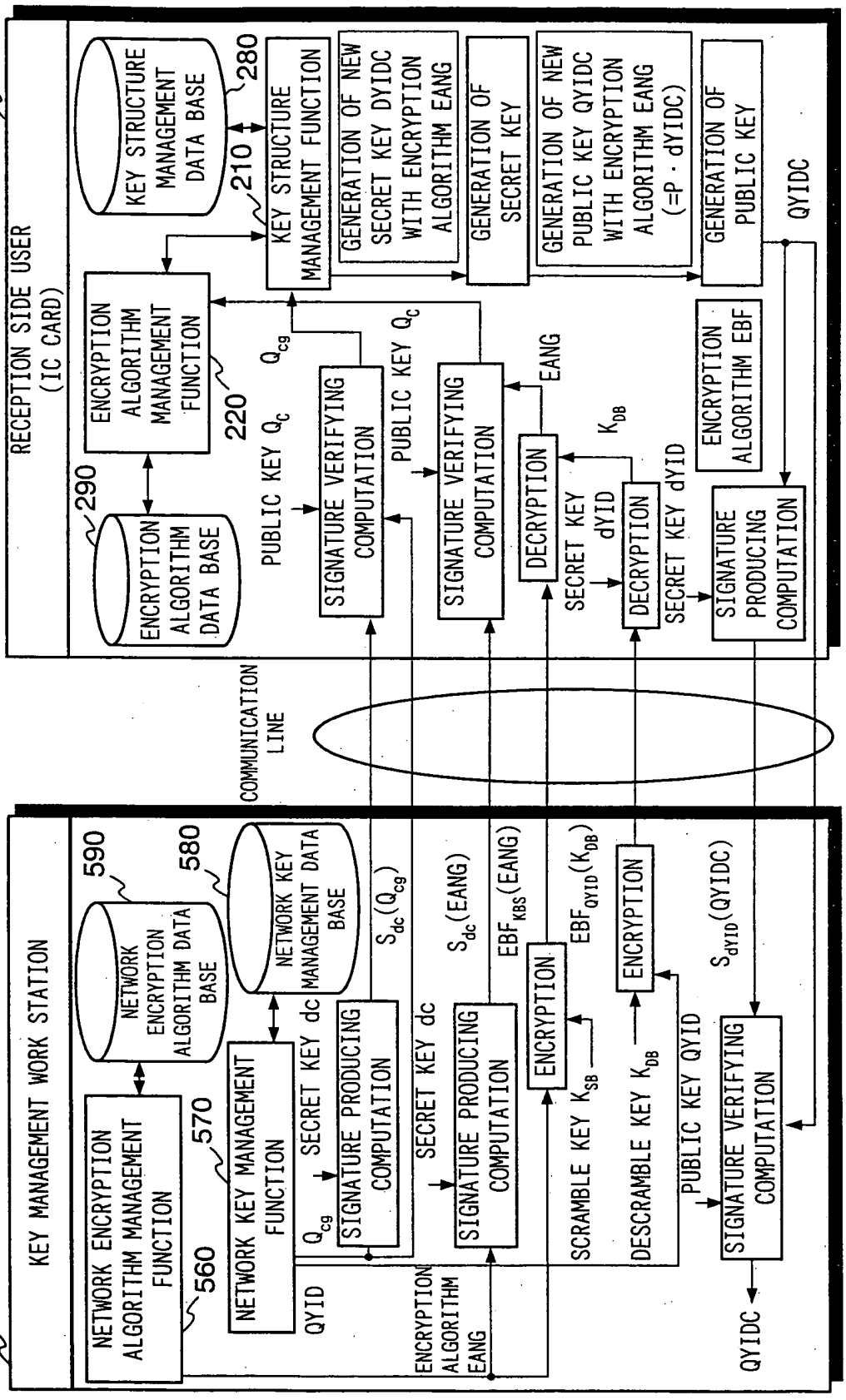


FIG. 21

(CRYPTOGRAPHIC COMMUNICATION SYSTEM WITH PUBLIC KEY ENCRYPTION ALGORITHM)

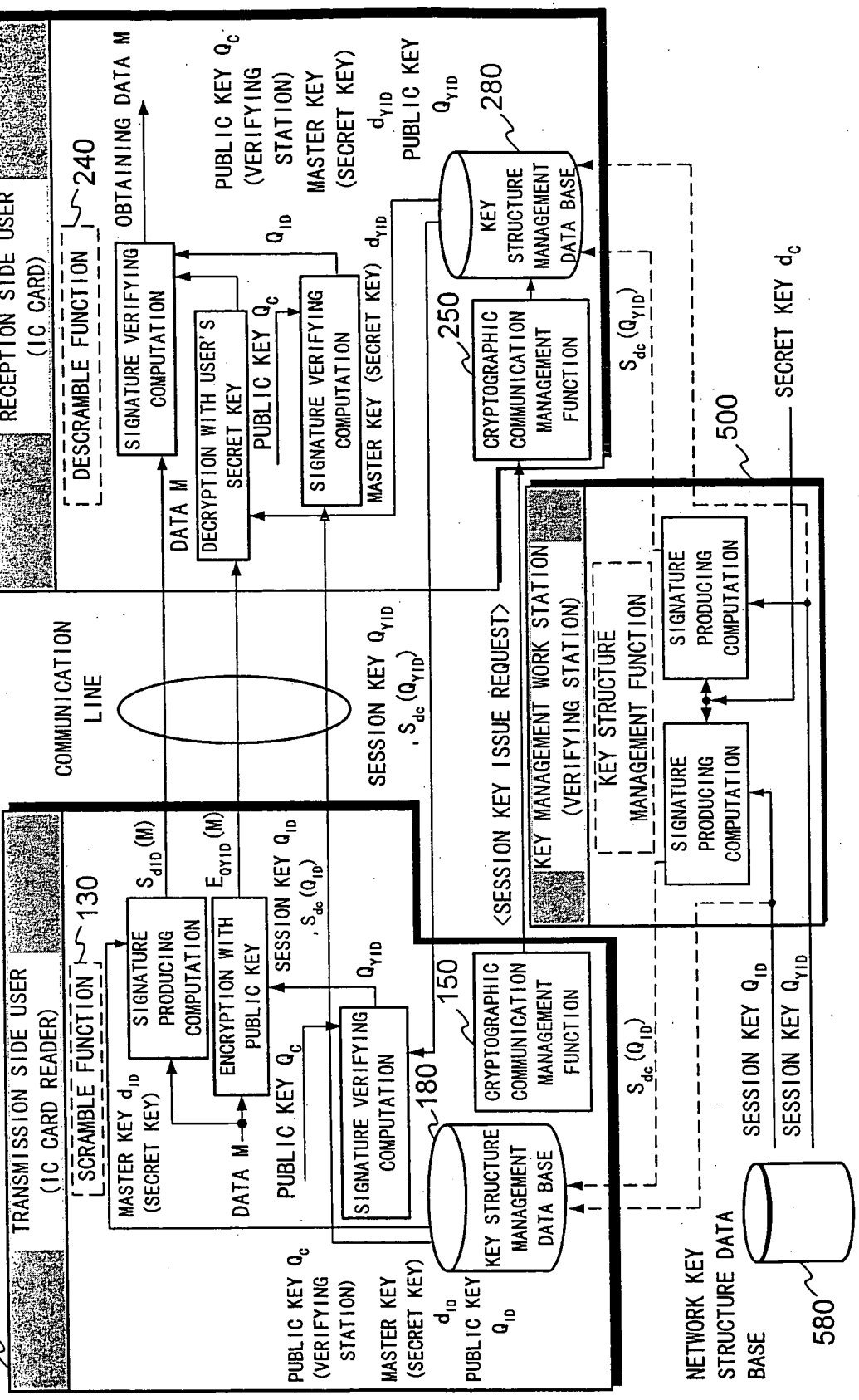


FIG. 22

(NETWORK COMMUNICATION SYSTEM
IN WHICH A PLURALITY OF ENCRYPTION ALGORITHMS EXIST)

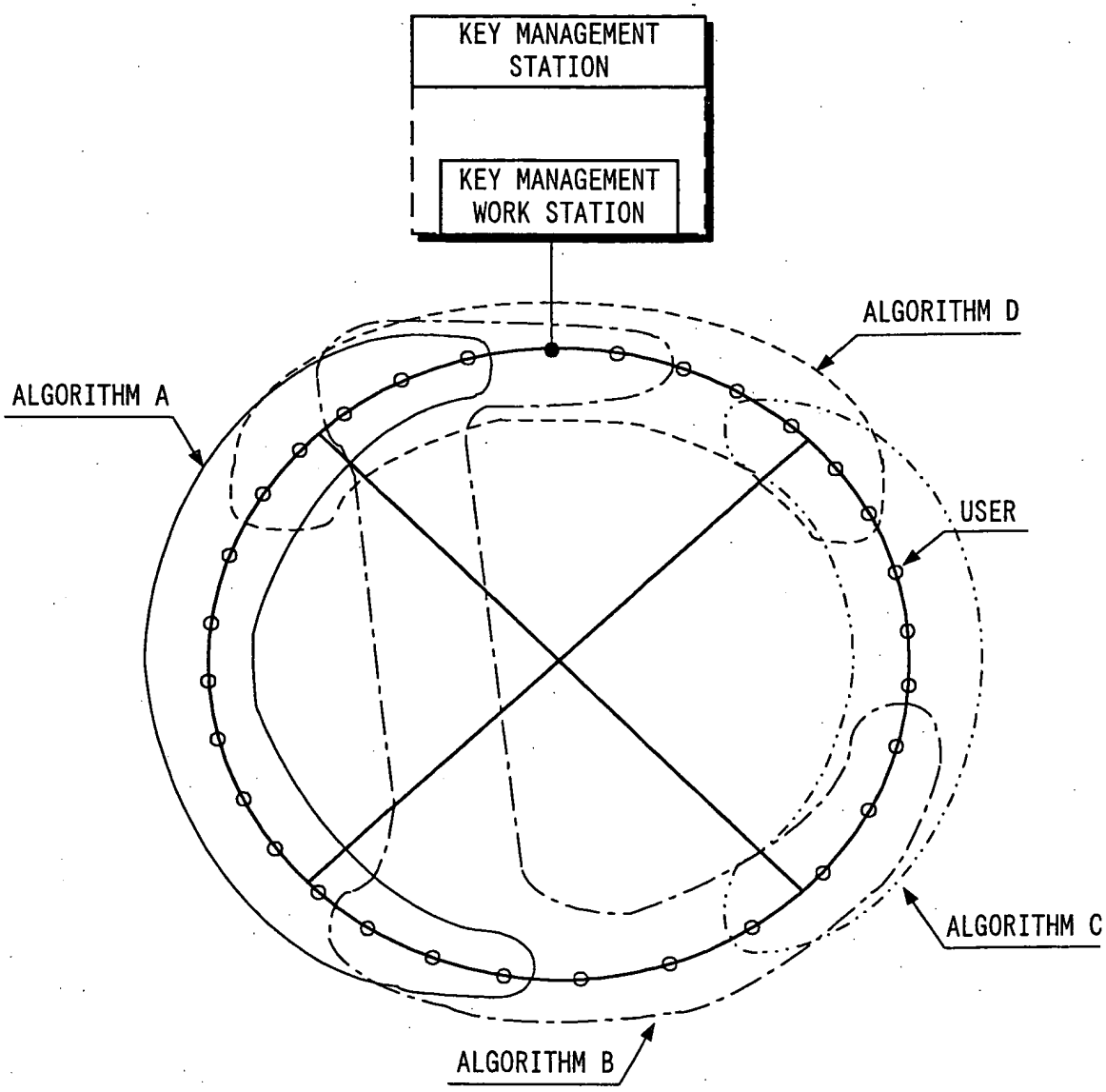


FIG. 23

(KEY RECOVERY FUNCTION (ENCRYPTION))

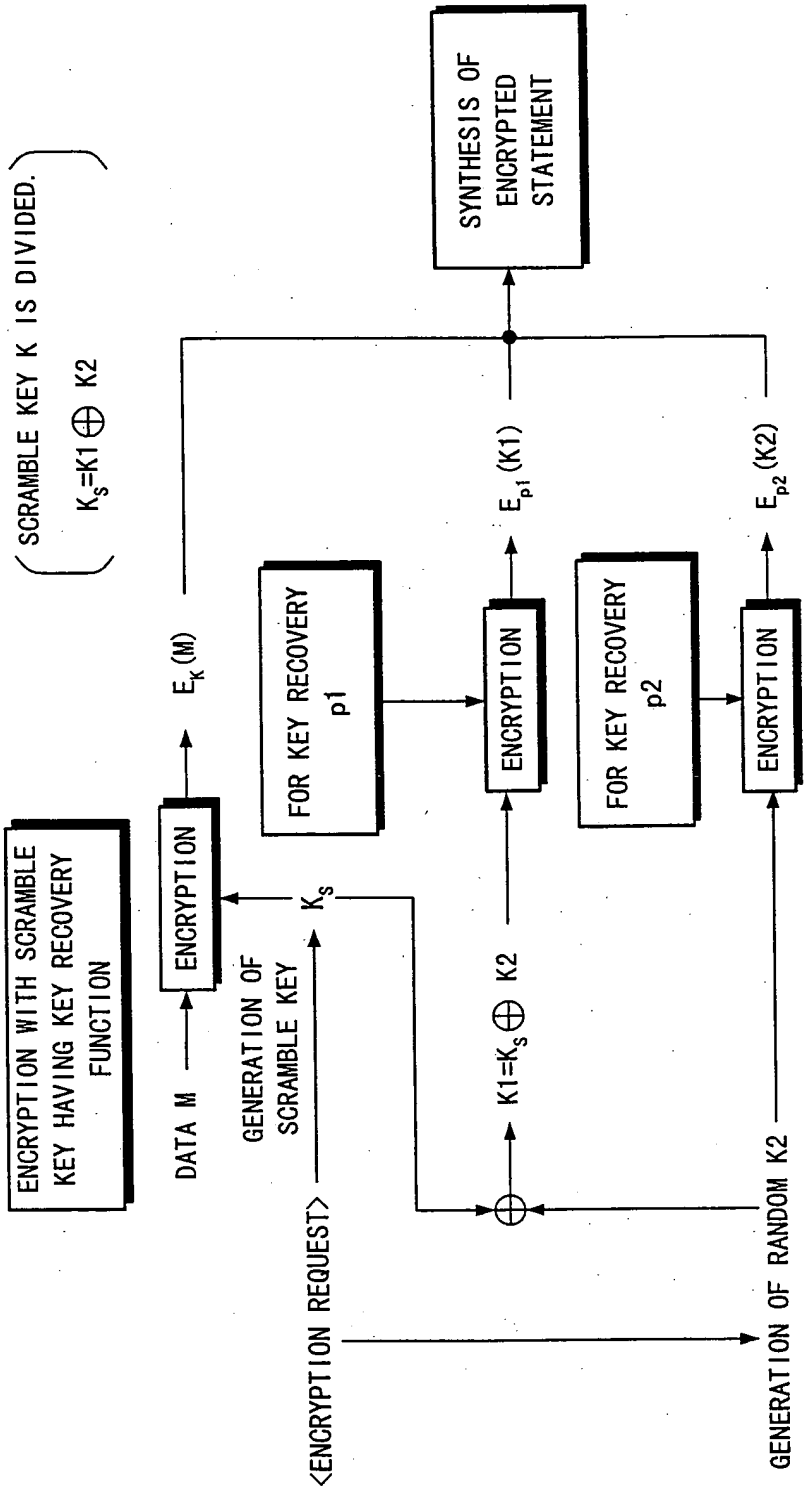


FIG. 24

(KEY RECOVERY FUNCTION (DECRYPTION))

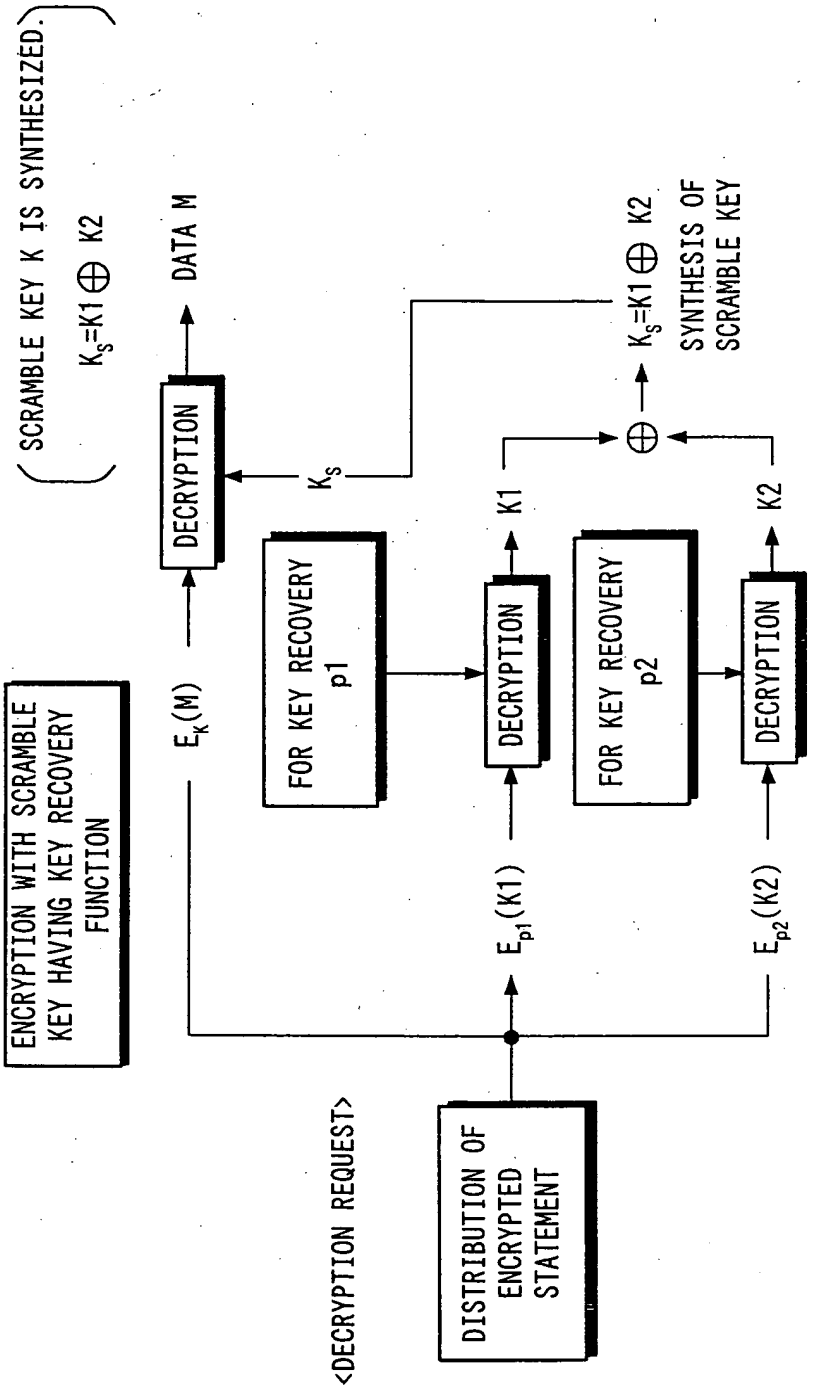
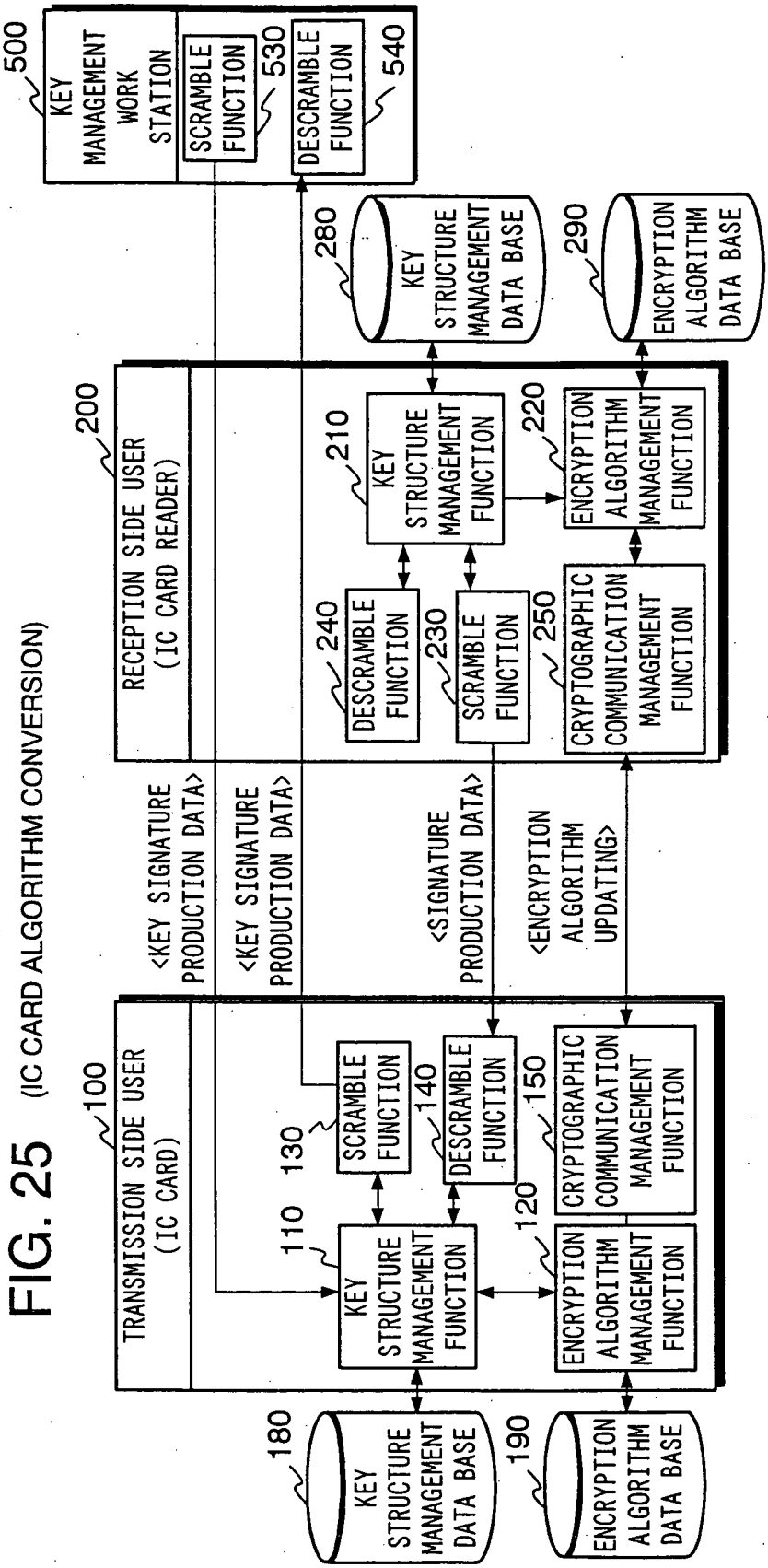



FIG. 25 (IC CARD ALGORITHM CONVERSION)